Security improvement in IoT based on Software Defined Networking (SDN)

Vandana C.P
Assistant Professor, New Horizon College of Engineering

***Abstract*— With the evolving Internet of Things (IoT) technology, there is exponential growth in connectivity of heterogeneous devices to the internet. Securing such complex heterogeneous networks and their diverse access protocols is a real challenge leading to security risk. Integration of Software Defined Networking (SDN) with IoT can open up way for better security and access control mechanisms.SDN is an intelligent networking paradigm which opens up vast opportunities to manage and secure IoT. In this paper, we have discussed the SDN based IoT architecture and have proposed a security framework for IoT based on SDN –IoT architecture.**

***Index Terms*— IoT, OpenFlow, SDN, SDN controller**

I. Introduction

With the ever growing internet and interconnection among everything, the need for security is a demand of the time. Internet of things (IoT) [1] which connects every object or device with networking capabilities is an area of great concern related to security. Objects include home automation sensors, medical equipments, vehicular sensors, nuclear reactors and any life critical real time sensing devices [2]. This means that lack of security in IoT can pose a risk to human lives.

IoT comprises of many heterogeneous devices which use diverse protocols. Each protocol follows different access mechanisms and security measures. But a unified security mechanism is still not in place in IoT.

Conventional security approaches like Intrusion Detection and Prevention Systems (IDPS), Firewall are deployed at internet edge devices to protect from external attacks. But in case of IOT which is seamless and borderless network access control become more difficult.

Software Defined Networking (SDN) [3] which is the new intelligent networking paradigm provides opportunities to solve issues related to IoT. By applying SDN network configuration and management can be simplified significantly. Industries wide acceptance for SDN shows that SDN can establish a tighter connection within the ecosystem of IoT.

In this paper, we discuss the current state of IoT, security challenges in IoT. We describe the need for SDN and its evolution. Further we analyze architecture of IoT based on SDN. Finally a security framework has been proposed based on SDN-IoT architecture.

II. Internet of Things (IoT)

A formal definition of IoT is given "A world where physical objects are seamlessly integrated into the information network and where the physical objects can become active participants in business process." as per [1]. Things can vary from physical objects to virtual objects which can be uniquely identified and connected via Internet. IoT consist of broad interconnection of several heterogeneous networks like wired, wireless, adhoc etc, each comprising of heterogeneous devices and environment, protocols employed by them for connectivity.

IoT structure can be broadly divided into 3 layers:

- **Perception layer** is responsible for sensing and collecting the data from the physical world and human worlds in IOT. Because of this functionality, it forms the core layer of the Internet of things. Things identification and intelligent acquisition is the main functionality. RFID devices, sensor devices, GPS, camera enabled devices comprises the perception layer.
- **Network layer** is responsible for information exchange and data transfer.
- **Application layer** provides human-machine interface and information processing layer. Currently, M2M (Man to Machine) is the most commonly used application form of the Internet of things.

A. Current State of IoT

To make IoT feasible, a reliable adaptation to the common protocols used in the networking environment of IoT should be built. The role of IP for the Internet is significant and is proposed as the solution for IoT, especially with the advancement of IPv6. However, in real world, this approach has lot of challenges and drawbacks related to heterogeneity of the devices and networks involved in IOT.

These objects and their protocols follow specific designs to meet specific user objectives. Trying to fit all these diversities of the objects into a common singular protocol is not a good option.

On the other hand, the Software Defined Networking (SDN) approach focuses on the programmability of all network elements. In this process, the control and data plane are separated in routing devices whereby the intermediate network devices functionality has been simplified to mere packet forwarding. A general control plane defines the forwarding rules for these simplified intermediate devices.

ISSN: 2278 – 7798

SDN ensures a promising future for IoT in terms of its feasible real world adaptation.

B. Security challenges in IoT

Due to the heterogeneity and complexity of the objects and networks in IoT, traditional authentication and authorization methods may not be applicable. Also the resource constrained devices in IoT restrict the usage of complex security mechanism. Some of the security challenges in the area of IoT are discussed.

a. Object Identification

The object identification is a challenging area in IoT. The Domain Name System (DNS) provides name translation services to Internet users which are vulnerable to attacks, like DNS cache poisoning attack, man-in-the-middle attack. Domain Name Service Security Extension (DNSSEC) as per IETF RFC4033 is deployed as the security extensions of DNS[6]. But it is still challenging to deploy DNSSEC in IOT due to its high communication overhead.

b. Privacy and Integrity

Data sensed by various physical nodes in IoT needs to be collected and anonymized. Encryption and decryption of the data needs to be performed. The resource constrained devices like sensor nodes in IOT are incapable to perform such complex security cryptographic operations creating loopholes in data privacy and integrity.

c. Authentication and Authorization

The traditional public-key cryptosystems cannot fit in IoT ecosystem. Authenticating and authorization through cryptographically pre-shared keys is not applicable. The rapidly growing number of objects will make the key management a difficult task in IoT. Lack of a global certification authority CA in the IoT is the main hindrance. The cryptographic algorithms are normally heavy and require huge memory prints restricting their usage in memory constrained devices in IoT.

d. Malware in IoT

The real time scanning performed by antivirus software is a great overhead in IoT devices. Recently, Symantec confirmed the existence of the first IoT malware, Linux, Darlloz, which marked the introduction of malware issue for IoT security. The real-time scanning functionality of antivirus may results in unaffordable overhead to IoT devices. Threat via malware in IoT is an area of great challenge and is an open research area.

III. SOFTWARE DEFINED NETWORKING (SDN)

In today's world of dynamic requirements, the network state changes continuously and gets updated as per the changing need of the end customers. Network administrators and operators need to adjust network configuration accordingly. Traditional routers and switches have both control (makes decision related to traffic management) and data plane (actual mechanism for routing traffic to destinations) in one device. So, these devices become slow, expensive, inflexible, non-scalable and sticky. Operators employ external tools, network scripts to dynamically reconfigure these network devices. This leads to miss-configuration errors. Software Defined Networking SDN [3] was proposed to solve these problems which conventional network control paradigms faced.

Open Networking Foundation (ONF) [4] is an organization dedicated to the promotion and adoption of SDN through open standards development.SDN is an intelligent architecture for network programmability by providing network abstraction. It decouples the control plane from the data plane, to provide programmability to the network.

As shown in Fig 1, SDN moves the control plane outside the switches. It enables an external centralized control of data through a logical software entity known as the SDN controller. SDN decouples software from hardware.SDN centralizes network state in the control layer. This makes the network management, provisioning, configuration, resource optimization and network security flexible using automated SDN programs. SDN architecture includes a set of API (Application Programming Interface) that supports the implementation of common network services like device discovery, address allocation and mapping, security, routing, access control, bandwidth allocation and resource optimization, energy usage management, storage support, QOS and other business related services.

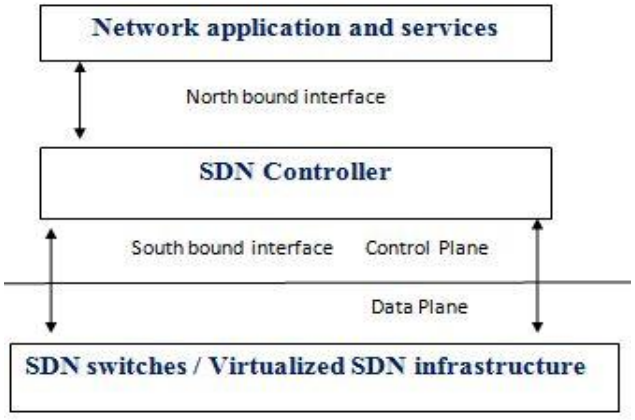

Fig1. SDN concept

As per SDN paradigm, the SDN controller establishes connection to the switch through OpenFlow Protocol [5]. The control plane is executed on individual off-the-rack equipment like PC and is also known as Open Flow Controller as shown in Fig 2.

Controller can update, add/delete the flow entries in the flow table either reactively in response to packets or proactively using predefined rules. The controller interface can be executed on any vendor hardware and operating system with high performance. The data plane is executed on dumb (no Layer2, Layer3 intelligence), powerful switches known as Open Flow Switch to forward data at line rate. The

ISSN: 2278 – 7798

topology can have a single SDN controller managing one or more switches, or a single switch controlled by multiple controllers.

SDN OpenFlow[5] provides northbound interface which is the high level interaction between controller and network application/services. The southbound interface is the lower layer interactions between controller and devices such as switches.

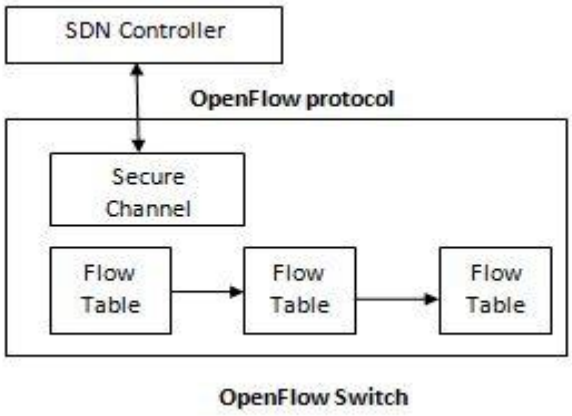

Fig 2. SDN capable Switch

Currently, SDN is employed in DCN [11][12] to gather bandwidth consumption data from nodes connected with fast network within the datacenter. The statistics collected includes link utilization also.

In IoT controller needs to gather state information from highly heterogeneous network and distributed network.IOT traffic data will be time sensitive and real time data. There should be provision to reduce collection overhead. Delay, jitter, packet loss, throughput are the statistics collected in IoT unlike DCN.

IV. IoT BASED ON SDN

As discussed in previous section, currently the SDN can be used as an overlay for IoT adaptation into the real world. The Fig 3 discusses architecture for IoT based on SDN. Any object in IoT can inter connect with any other object via the SDN capable network as shown in figure3. Each IoT device has an IoT agent which interacts with IoT controller.

IoT agent is responsible to sense, analyze and collect the data from the environment to achieve the user objectives. All the IoT agents needs to be registered with the IoT controller with the details like its object identifier, address, communicating network protocol and underlying network.

IoT controller will take the necessary decisions based on the data provided to it by the IOT agents. These decisions are reflected to the underlying physical network via the SDN controller. IoT controller on receiving the connection request from its IoT agent will build the forwarding rules depending on the networking protocols used, and communicate these rules to the SDN controller.

Once the IoT controller receives the destination objects' address or identifier, it needs to find it in the network. This is easy because IoT agents will be registered with the IoT controller and they provide their corresponding identifier or address.

SDN controller establishes the network path that connects both objects by running a routing algorithm with topology information from both IoT and SDN levels.

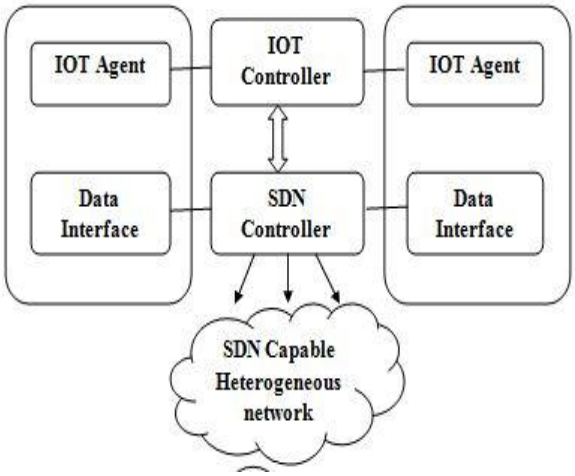

Fig 3. SDN based IOT Architecture

V. RELATED WORK

The SDN controller can not only mange the IoT heterogeneous network but can also monitor the incoming and outgoing traffic. SDN controller can efficiently secure the IoT network from inside and outside attack.

Much research work has been done to provide security by implementing firewalls, IPS and IDS on top of the SDN controller [6], [7], [8]. Security policies are installed into OpenFlow switches [5]. However, authenticating network devices, users and objects connecting to users using both heterogeneous technologies in IoT is not yet at place.

Solution using one single SDN controller: Security frameworks based on a single SDN controlled are discussed in previous works [10], [13], [14], [15]. Denial of service (DOS) attack can occur at the SDN controller which is the single point of failure. If an internal attack occurs and compromises the SDN controller, then full control over the network can be taken.

Solution using multiple SDN controllers: In [16], it is observed that multiple controllers can increase trustworthiness and fault tolerance. When one of the SDN controllers fails, another controller can take control to overcome system failures. But there is decrease in network performance with multiple controllers. Since each controller has a partial view of the network, controllers need to collaborate with each other and exchange information creating overhead.

VI. PROPOSED SECURITY FRAMEWORK

IoT compromises of many resource constrained devices like sensor nodes. Hence it is not possible that each device is SDN capable. However, each IOT device will have an IoT

ISSN: 2278 – 7798

agent and IoT controller as discussed in section 4. We assume that such resource constrained device can be associated to one neighbor node which is SDN capable.

We segment the heterogeneous network of IoT into various segments as shown in Fig 4. In each segment there will be resource constrained devices like senor nodes, mobile nodes, smart object etc. Also there will be devices which have enough resources and are SDN capable. These are OpenFlow capable nodes. These resource constrained nodes needs to be associated with OpenFlow capable nodes in their segment. Each segment has its SDN controller which controls all the traffic in that segment. These Open Flow capable nodes must be connected to its segment's SDN controller.

The job of the SDN controller in each segment is to authenticate the network devices. After successful establishment of Open Flow secure connection between the switch and the controller, the controller blocks switch ports directly connected to the users. Once the user is authenticated, based on user authorization level the SDN controller will enable the corresponding flow entries to the switch.

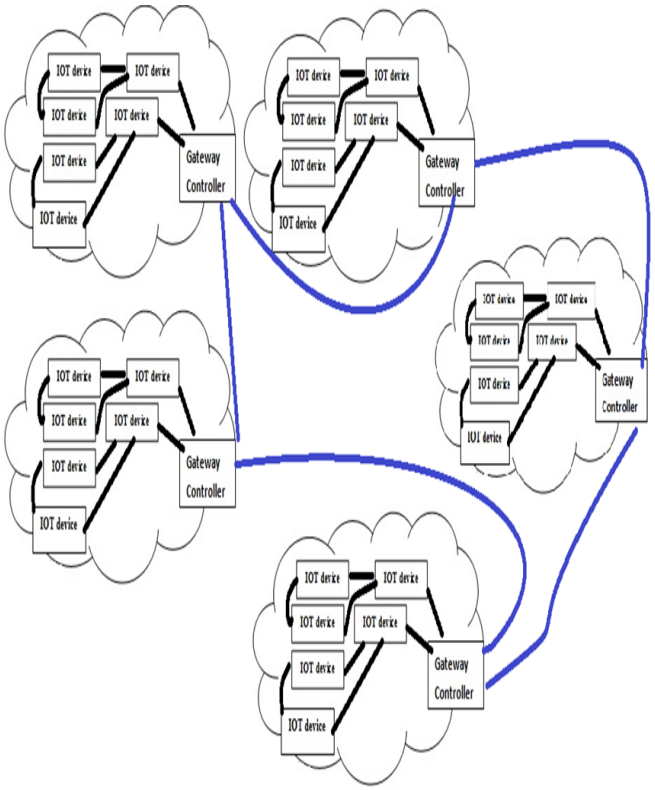

Fig 4. SDN Segment and security mechanism

Each controller of each segment exchanges their security rules. SDN controllers now behave as security guards on the edge of the network segment. An SDN controller provisions safety connections between segments and accepts only authorized traffic. When a node wants to communicate with another node of another segment, the flow has to be forwarded to the SDN Controller, also called the Gateway Controller. The Gateway controller sends request to each of its neighbor Gateway controller to check if it knows the destination address of this data. Only services authorized by controller can be used for endpoint devices.

For example, a File Transfer channel has to be established by one device to another. So device will request its SDN controller in its segment to authenticate its user request and corresponding traffic. Once authorized, the SDN controller establishes the flow entries and sends the traffic to the Gateway controller. The Gateway controller then sends request to its neighboring controllers to determine if the destination address exit in their respective segments.

The destination Gateway Controller carries of the same authentication procedure in its destination device segment.Only the authorized devices can communicate with the Gateway controller at destination segment. If the intended recipient is not present, then appropriate response is sent back to the source Gateway Controller.

Thus SDN based IoT architecture can be employed to establish security frameworks. The traditional heavy cryptographic techniques are not required to be installed on resource constrained devices in IoT. Instead SDN controllers can play a vital role in ensuring the security. In a distributed environment, the Gateway Controllers will ensure the authorization and enforce security.

VII. Conclusion and Future Work

The scope of SDN in IoT to provide solution for various challenges is discussed. The various security issues in IoT are analyzed. A framework to improve the security in IoT based on SDN architecture has been proposed.

In future, the proposed framework will be implemented and its security effectiveness will be measured. The DOS attack would be simulated in the IoT and the efficiency of the proposed framework to prevent DOS attack would be computed.

REFERENCES

[1] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in Future Internet – FIS 2008 Lecture Notes in Computer Science Vol. 5468, 2009, pp 14-28.

[2] A. C. Sarma, and J. Girão, "Identities in the Future Internet of Things," in Wireless Personal Communications 49.3, 2009, pp. 353-363.

[3] "Software defined networking: Definition", Website, https://www.opennetworking.org/sdn-resources/sdn-definition.

[4] "Open network foundation", Website, https://www.opennetworking.org/about/onf-overview.

[5] "Open flow spec 1.3," https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf.

[6] S. Scott-Hayward, G. OCallaghan, and S. Sezer, "SSDN security: A survey", in Proceedings of the IEEE SDN for Future Networks and Services. pp.1-7, 2013.

[7] S. Son, S. Shin, V. Yegneswaran, P. Porras, and G.Gu, "Model checking invariant security properties in openflow", in Proceedings of the IEEE International Conference on Communications. pp. 1974-1979, 2013.

[8] H. Hu, W. Han, G.J. Ahn, and Z. Zhao, "Flowguard: Building robust firewalls for software-defined networks", in Proceedings of the Third Workshop on Hot Topics in Software Defined Networking. pp. 97–102, 2014.

[9] R. Jin and B. Wang, "Malware detection for mobile devices using software defined networking", in Proceedings of the Workshop of Research and Educational. pp. 81-88, 2013.

[10] R. Skowyra, S. Bahargam, and A. Bestavros, "Software-defined ids for securing embedded mobile devices", in Proceedings of the Workshop of Research and Educational. pp. 84-48, 2014.

[11]A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, "Devoflow: scaling flow management for high-performance networks," in Proceedings of the ACM SIGCOMM 2011 conference, ser.SIGCOMM '11, 2011.

[12] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: dynamic flow scheduling for data center

ISSN: 2278 – 7798

networks," in Proceedings of the 7th USENIX conference on Networked systems design and implementation, ser. NSDI'10, 2010.
[13] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," SIGCOMM Computer Commununication.
[14] M. Mendonc¸a, B. N. Astuto, X. N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," IEEE 37th Conference on. IEEE, 2013, pp. 311–315.
[15] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOXIOpenFlow, in Local Computer Networks (LCN)",2010 IEEE 35th Conference on. IEEE, 2010, pp. 408–415.
[16] H. Jafarian, E. Al-Shaer, and Q. Duan, "Open flow random host mutation: transparent moving target defense using software defined networking", in Proceedings of the first workshop on Hot topics in software defined networks, ACM, 2012, pp. 127–132.

Vandana C.P is currently working as Assistant Professor in Information Science and Engineering department, New Horizon College of Engineering. She has pursued her Masters in Computer Network Engineering from VTU. She has 6 years of software industry experience and 2yrs teaching experience. She has worked in telecom domain mainly on network management systems (NMS) and storage area networks (SAN) domain. Her research interest includes security issues in MANET, VANET, network management systems and functionalities.

ISSN: 2278 – 7798